VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Čítání osob na základě analýzy WiFi provozu

People Counter Based on WiFi Signal Analysis

2019 Tomáš Klubal

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Tomáš Klubal**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: Čítání osob na základě analýzy WiFi provozu
People Counter Based on WiFi Signal Analysis

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem bakalářské práce je navrhnout a otestovat software umožňující odhadnout počet osob v blízkosti přijímače na základě pasivní analýzy WiFi signálů. Navržená aplikace bude pomocí vhodné utility (např. Wireshark, tcpdump) odposlouchávat tzv. Beacon frames, které vysílají přístupové body, provoz generovaný klienty a analyzovat jejich obsah. Na základě analýzy výskytu jednotlivých unikátních MAC adres se algoritmus pokusí odhadnout počet zařízení (osob), které se nacházejí v rádiovém dosahu přijímače.

1. Proveďte rešerši pasivních metod určování počtu osob na základě analýzy rádiového pásma (zaměřte se na mobilní sítě a WiFi).
2. Navrhněte a implementujte aplikaci, která bude provádět sběr a analýzu dat z bezdrátového adaptéru.
3. Vytvořte algoritmus, který na základě výskytu jednotlivých MAC adres odhadne počet aktivních zařízení.
4. Navrhněte a implementujte vhodnou metodu zobrazování výsledků.
5. Navržené řešení otestujte a výsledky shrňte v závěru práce.

Seznam doporučené odborné literatury:

[1] Andrew S. Tanenbaum, David J. Wetherall : Computer Networks, Pearson; 5 edition, 2010, ISBN 0132126958
[2] Chris McNab, Network Security Assessment: Know Your Network, O'Reilly Media; 3 edition, 2016, ISBN 978-1491910955
[3] Matthew S. Gast: 802.11 Wireless Networks: The Definitive Guide, Second Edition, O'Reilly Media; 2 edition, 2005, ISBN 0596100523

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Mgr. Ing. Michal Krumnikl, Ph.D.**

Datum zadání: 01.09.2018

Datum odevzdání: 30.04.2019

doc. Ing. Jan Platoš, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 26. dubna 2019 .....

Rád bych tímto poděkoval Mgr. Ing. Michalu Krumniklovi, vedoucímu bakalářské práce, za odborné vedení při zpracovávání bakalářské práce a za zapůjčení technického vybavení.

Abstrakt

V bakalářské práci se věnuji vývoji softwarové aplikace, která z analýzy WiFi provozu odhadne počet osob v rádiovém dosahu přijímače. V teoretické části práce popisuji technické pojmy a základní teorie potřebné k objasnění způsobu fungování bakalářské aplikace. V praktické části práce se věnuji tvorbě vlastní aplikace a jejímu testování.

Klíčová slova: čítání osob, Python, WiFi, Pcapy, DPKT, MAC hlavička, WiFi rámce

Abstract

The bachelor thesis deals with the development of a software application that estimates the number of people within radio range of the device from the WiFi traffic analysis. In the theoretical part I describe technical terms and basic theories needed to clarify the way of bachelor application. In the practical part of my thesis I write my own application and test it.

Key Words: people couting, Python, WiFi, Pcapy, DPKT, MAC header, WiFi frame

Obsah

Seznam použitých zkratek a symbolů

AP	–	Access point
IMSI	–	International Mobile Subscriber Identity
MAC	–	Media Access Control address
NIC	–	Network Interface Controller
OUI	–	Organizationally Unique Identifier
QoS	–	Quality of Service
RB	–	RouterBOARD
SSID	–	Service Set IDentifier
TCP/IP	–	Transmission Control Protocol/Internet Protocol

Seznam obrázků

Seznam tabulek

Seznam výpisů zdrojového kódu

1 Úvod

Požadavek na čítání osob v daném prostoru vznikl již v minulosti. Dříve se počet osob v daném prostoru zjišťoval různými metodami od prostého počítání osob až po odborné odhady. V současné době je možné stanovit počet osob v daném prostoru pomocí informačních technologií. Jednou z metod je čítání osob pomocí analýzy obrazu (např. detekce obličeje). Počet osob v daném prostoru se dá stanovit také na základě analýzy WiFi provozu nebo mobilních sítí. Většina těchto aplikací funguje za předpokladu, že každá osoba ve sledovaném prostoru má u sebe právě jedno WiFi zařízení. Z tohoto předpokladu vychází i má bakalářská práce.

Pro svou bakalářskou práci jsem si zvolil téma 'Čítání osob na základě analýzy WiFi provozu'. Ve své práci si kladu za cíl navrhnout a otestovat softwarovou aplikaci vytvořenou za účelem odhadnutí počtu osob v rádiovém dosahu přijímače na základě pasivní analýzy WiFi signálu. Téma bakalářské práce mne zaujalo především z toho důvodu, že se dá předpokládat využití bakalářské aplikace v praxi. Aplikace by mohla najít využití např. v případech, kdy je potřeba znát přibližný počet procházejících osob v obchodním domě, počet účastníků na přednášce nebo intenzitu využití daného prostoru.

V úvodu bakalářské práce se budu věnovat popisu fungování metody čítání osob na základě pasivní analýzy WiFi provozu. Poté je nutné se seznámit s technickými pojmy a základními teoriemi potřebnými k vysvětlení a pochopení způsobu fungování bakalářské aplikace. Provedu rešerši některých produktů na čítání osob a sledování jejich polohy pomocí pasivní analýzi WiFi provozu, které již byli uvedeny na trh, zda se jedná o komerční či nekomerční produkty nebo zda některé z nichž umožňují uživatelům využit i další funkce nesouvisející s čítáním osob.

Vlastní aplikaci se budu věnovat v kapitole č. 4 Popis aplikace, a to sběru dat, zpracování a analýze dat. Z důvodu zpřesnění výsledků aplikace v odhadu počtu osob v rádiovém dosahu přijímače bych chtěl uživateli implementovat do aplikace možnost výběru několika parametrů. Volbou vhodných parametrů by došlo k odfiltrovaní WiFi rámců vysílaných z nežádoucích a vyloučených zařízení. Tím by mělo dojít ke zpřesnění výsledků aplikace. Z důvodu přehlednosti se pokusím výstupy vygenerovat do grafů, které budou prezentovat výsledky skenování WiFi provozu z různých hledisek. Zároveň zvažuji vytvoření šablony, která by tyto grafy generovala do protokolu. V bakalářské práci uvedu postupy pro instalaci bakalářské aplikace a její spuštění. Bakalářskou aplikaci plánuji otestovat provedením několika testů, které bakalářskou aplikaci prověří z několika hledisek.

Očekávané a dosažené výsledky bakalářské aplikace porovnám v závěru své bakalářské práce.

2 Technický rozbor

Cílem mé bakalářské práce je navrhnout a otestovat softwarovou aplikaci vytvořenou za účelem odhadnutí počtu osob v rádiovém dosahu přijímače na základě pasivní analýzy WiFi signálu.

Pasivní metody určování přibližného počtu osob pracují na základně pasivního sledování rádiového pásma, tzn. že signály jsou pouze přijímány. Sledováním provozu mobilní sítě můžeme zjistit počet osob odchytáváním a analýzou GSM provozu. Tato metoda je založena na skutečnosti, že každý mobilní telefon má unikátní identifikační číslo IMSI. Z tohoto čísla lze zjistit kód země, kód mobilního operátora nebo kód mobilního telefonu v síti mobilního operátora. Aplikace na čítání osob fungují na principu pasivního odchytávání GSM provozu a identifikace unikátního čísla IMSI v odchycených datech.[1]

Odhadnout počet osob lze také pasivním sledováním WiFi provozu na základě odchytávání WiFi rámců odeslaných zařízeními v okolí přijímače. S touto metodou pracuje moje bakalářská aplikace na čítání osob.

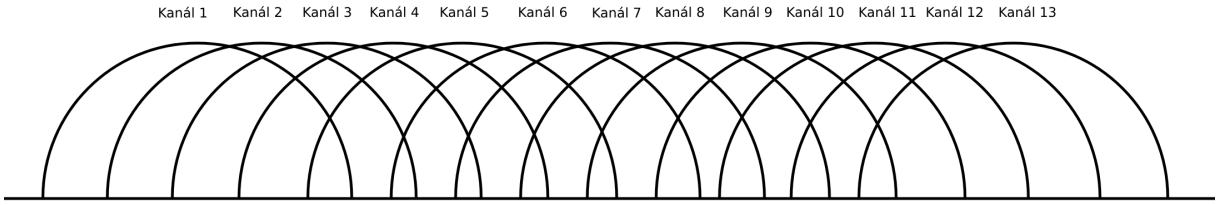
Před započetím práce na vlastním algoritmu je nutné se seznámit s některými technickými pojmy a postupy souvisejícími s odchytáváním WiFi signálů ze zařízení. Z tohoto důvodu se v této kapitole věnuji popisu základních technických pojmů a souvislostí v oblasti odchytávání WiFi rámců a také metodám jejich odchytávání, avšak pouze těm, které je potřeba znát pro pochopení bakalářské aplikace a způsobu jejího fungování.

2.1 Technologie WiFi

WiFi patří mezi technologie sloužící pro bezdrátové přenosy dat, která je provozována na frekvenčních pásmech 2,4 GHz a 5 GHz. Standard 802.11 dělí frekvenční pásmo do 13 kanálů (v některých zemích do 14 kanálů) vzájemně posunutých o 5 MHZ. Šířka jednoho kanálu je 20 MHz. Vzhledem ke skutečnosti, že je šířka kanálu větší než vzájemný odstup jednotlivých kanálů, dochází k vzájemnému překrývání kanálů. Takto se navzájem interferují např. kanály 1 až 5. Naopak kanály, které se navzájem neovlivňují jsou např. 1, 6 a 11. Překrytí jednotlivých kanálů přehledně znázorňuje obrázek č. 1. [2]

Popis fungování WiFi je uveden ve standardu 802.11. K tomuto základnímu standardu vychází postupně dodatky, které WiFi zkvalitňují nebo zrychlují. [3] Níže uvádím příklady některých dodatků:

- 802.11a – využití WiFi v pásmu 5 GHz
- 802.11b – zvýšení přenosové rychlost na 11 Mbit/s
- 802.11e – přidání podpory kvality služeb (QoS)
- 802.11ac – zvýšení přenosové rychlosti na 1 Gbps v pásmu 5 GHz



Obrázek 1: Zobrazení překrytí WiFi kanálů

- 802.11d – přidání podpory pro dodatečné informace do *beacons*, *probe requests* a *probe responses* (dle dodatečných informací z těchto WiFi rámců zařízení přizpůsobí např. frekvenci nebo vyzařovací výkon na požadovanou hodnotu).

2.2 MAC adresa

MAC adresa je unikátní označení sítového zařízení. Prezentována je skupinou šesti dvojic hexadecimálních číslic, které jsou nastaveny již od výrobce. MAC adresa se dá rozdělit na dvě části. První tři dvojce číslic (OUI) označují výrobce zařízení. Druhým třem dvojicím číslic (NIC) přiřadí hodnotu výrobce, a to tak, aby MAC adresa zařízení byla unikátní.

Původní záměr byl, že MAC adresa zařízení bude unikátní a neměnná. Protože WiFi zařízení při připojování nebo hledaní AP vysílá *probe-request*, který MAC adresu obsahuje, je tudíž snadné konkrétní WiFi zařízení lokalizovat a sledovat jeho pohyb. V dnešní době je však za jistých podmínek u některých zařízení MAC adresa náhodně měněna, a to právě z důvodu znesnadnění sledování pohybu konkrétního zařízení.[2][6]

S náhodným generováním MAC adresy pracuje operační systém Android od verze Android 8.0 Oreo.[8] Operační systém pracuje s náhodně vygenerovanou MAC adresou zařízení v případě, kdy není zařízení připojeno k WiFi síti. Od verze Android 9.0 Pie je již však možné zapnout v nastavení funkci generování náhodné adresy i při připojení zařízení k WiFi síti.

Co se týká operačního systému Windows je generování náhodné MAC adresy podporováno od verze Windows 10,[9] kdy je tato funkce v továrním nastavení standardně vypnuta. V případě potřeby je však možné ji zapnout. U operačního systému Linux je tato funkce podporována od kernelu 3.18.[10]

2.3 WiFi rámce

Tři druhy WiFi rámců jsou definovány od standardu IEEE802.11, a to *management frame*, *control frame* a *data*. Každý WiFi rámec se skládá z MAC hlavičky, *payload* a *frame check sequance* s tím, že *payload* není povinný.

Moje aplikace pro čítání osob pracuje jen s určitými daty z MAC hlavičky. Z tohoto důvodu se dále věnuji popisu pouze používaných částí MAC hlavičky.[2][6]

2.3.1 MAC hlavička

Na úvod uvádím, že MAC hlavička se skládá z několika hlavních fragmentů[2], které uvádím v tabulce č. 1.

Frame Control	Duration	Adress 1	Adress 2	Adress 3	Sequence Control	Adress 4	Frame Body	CRC

Tabulka 1: Struktura MAC hlavičky

Protože má bakalářská práce pracuje s dalšími fragmenty, ze kterých se *frame control* skládá, uvádím strukturu *frame control* v tabulce č. 2.

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd

Tabulka 2: Struktura frame control

- *Protocol Version* – indikuje, který protokol je používán
- *Type* – označuje, zda se jedná o *management frame*, *control frame* nebo *data frame*
- *Subtype* – specifikuje typ WiFi rámce jako například *beacon*, *disassociation*, *QoS Data*
- *To DS* – indikuje, zda WiFi rámec odeslal klient
- *From DS* – indikuje, zda WiFi rámec odeslalo *distribution system*
- *Retry* – indikuje, zda se v minulosti WiFi rámec již odeslal, ale stanice nezískala potvrzovací signál o jeho přijetí
- *Power Management* – indikuje, že stanice přechází do *Power Save* modu
- *Protected Frame* – indikuje, zda je *payload* datového WiFi rámce šifrován
- *Order* – indikuje požadavek na striktní uspořádání WiFi rámců, které musí být zpracovány v daném pořadí

Type rozlišuje rámce:

- *Managment Frame*
- *Control Frame*
- *Data Frame*

2.3.2 Management frame

Standard IEEE 802.11 definuje[2]:

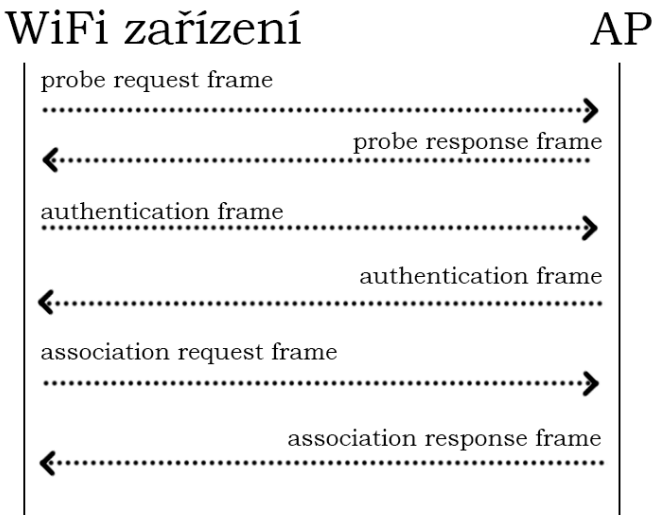
- *Authentication frame* – WiFi rámec odesílaný během připojování do WiFi sítě
- *Association request frame* – WiFi rámec odesílaný stanicí, který obsahuje informaci o síťovém zařízení a SSID sítě, do které se chce zařízení připojit
- *Association response frame* – stanici zaslaná odpověď na její žádost (*association request frame*); žádost může být zamítnuta nebo schválena
- *Beacon frame* – WiFi rámec odesílaný z AP, který obsahuje informace o jeho bezdrátové síti
- *Deauthentication frame* – WiFi rámec označující, že stanice ukončuje spojení s jinou stanicí
- *Disassociation frame* – WiFi rámec označující, že stanice ukončuje spojení s jinou stanicí; oproti *Deauthentication frame* umožňuje přístupovému bodu uvolnit prostředky pro jinou stanici
- *Probe request frame* – WiFi rámec odesílaný stanicí, která žádá informace od jiných stanic
- *Probe response frame* – odpověď na *probe request frame*
- *Reassociation request frame* – pokud dojde k poklesu signálu pod hranici spolehlivého přenosu, síťové zařízení zašle tento *frame* a bude hledat přístupový bod se silnějším signálem
- *Reassociation response frame* – WiFi rámec s odpovědí přístupového bodu na *reassociation request frame*

2.4 Metody vyhledávání bezdrátových sítí

Pokud sítový adaptér vyhledává dostupné AP sítě, využije přitom jednu ze dvou hlavních metod.[4][7]

2.4.1 Metoda 1

Při této metodě pracuje sítový adaptér pasivně, a to tak, že odchytává tzv. *beacon frame*, ze kterých získá informace o bezdrátových sítích. Síťový adaptér v danou chvíli skenuje *beacon frame* vždy na jednom kanále a po určitém časovém intervalu přechází na další kanál. Pokud má AP svoji WiFi síť skrytou, není *beacon frame* vysílán. Pasivní skenování všech WiFi kanálů je časově náročné. Při této metodě je také vyšší spotřeba energie.



Obrázek 2: Znázornění inicializace připojení k WiFi síti

2.4.2 Metoda 2

Druhá metoda pracuje na bázi aktivního skenování WiFi kanálů, tzn. že síťový adaptér signály přijímá i vysílá. Síťový adaptér odešle na konkrétním kanále *probe-request frame* a poté přijímá odpovědi *probe response frame* od AP. Výhodou této metody je kratší skenovací čas (po odeslání *probe-request frame*), což se promítne v menší spotřebě energie než u první metody.

V praxi se tyto dvě metody obvykle kombinují, tzn. že zařízení po zapnutí WiFi začne odposlouchávat *beacon frame* o dostupných WiFi sítích a zároveň odešle *probe request frame*, na základě které mu AP zašle *probe response frame*. Pokud zařízení nalezne WiFi síť, na kterou se chce připojit, vyšle *authentication frame*, na který mu konkrétní AP zašle *authentication frame*. Nakonec zařízení odesílá *association request frame*, AP bod odešle *association response frame*. V tuto chvíli je zařízení připojeno k požadované WiFi síti. Inicializace připojení k WiFi síti je znázorněna v obrázku č. 2.[5]

3 Dostupné aplikace

V praxi se v případě potřeby elektronického čítání osob nebo sledování jejich pohybu používají aplikace a nástroje, které fungují na principu skenování WiFi kanálů, odchytu WiFi provozu a vyhodnocování zachycených WiFi rámců. Níže uvádím příklady aplikací a nástrojů na elektronické čítání osob nebo sledování jejich pohybu, z nichž některé nabízejí možnost využít i další funkce. Všechny aplikace a nástroje však pracují pouze se zařízením s WiFi signálem.

3.1 Accuware WiFi Location Monitor

Accuware WiFi Location Monitor je systém pro sledování zařízení s podporou WiFi technologie v reálném čase. Princip fungování tohoto systému je založen na pasivním skenování WiFi provozu a jeho analýze. Pro funkčnost tohoto systému je potřeba rozmístit po monitorovaném prostoru výrobcem dodávané *nodes*. *Node* je specifické zařízení, které odchytává WiFi provoz, zaznamenává MAC adresy a sílu WiFi signálu. Tyto údaje periodicky odesílá na server, který poté odhadne polohu zařízení na základě dat ze všech *nodes*. Pro správné určení polohy zařízení je však nutné nejdříve nahrát na server plán monitorovaného prostoru s označením umístění jednotlivých *nodes* a jejich identifikace. Součástí tohoto produktu je výstup v podobě detailní zprávy výsledků, ze které je možné vyčíst např. informace, zda se návštěvník v monitorovaném prostoru vyskytl poprvé nebo monitorovaný prostor již v minulosti navštívil. Ve výsledcích je rovněž možné nalézt počet unikátních MAC adres, analýzu návštěvnosti nejen v reálném čase, ale také historicky, nebo tzv. teplotní mapu hustoty osob nacházejících se v monitorovaném prostoru. Protože tento systém pracuje pouze se zařízením se zapnutou WiFi, nejsou do počtu osob v monitorovaném prostoru započítávány osoby se zařízením s vypnutou WiFi. Tím dochází ke zkreslení výsledků. Z důvodu přesnějších výsledků počtu osob bývá v monitorovaném prostoru nabízena *free* WiFi za účelem zapnutí WiFi na co největším počtu zařízení, čímž dojde k odchytávání WiFi rámců z více zařízení. Pro používání systému Accuware WiFi Location Monitor je nutné zakoupit licenci.

3.2 FIND

Framework for Internal Navigation and Discovery umožňuje používání zařízení s WiFi technologií pro zjištění polohy WiFi zařízení v domě a následnou automatizaci. Systém se skládá ze dvou komponent. První komponentou je zařízení, které skenuje WiFi provoz v monitorovaném prostoru a poté na server odesílá získané MAC adresy a síly signálu. Druhou komponentou je server se strojovým učením, který přijatá data následně zpracovává. Hlavní myšlenka projektu spočívá ve snaze o co nejjednodušší automatizaci objektu s minimálními náklady, přičemž nedojde k použití například pohybových senzorů. Jako příklad bych uvedl využití tohoto systému u ovládání lampy u příjezdu k domu. Pokud je ovládání lampy řízeno senzorem pohybu, bude lampa rozsvěcována při každém detekovaném pohybu. V případě použití systému FIND dojde

k rozsvícení lampy pouze v případě, že server bude detekovat osobu s WiFi zařízením, které má oprávnění lampu rozsvítit. Dle mého názoru je výhodou systému FIND přizpůsobení serveru pro použití na Raspberry Pi model B+. Jako sledovací zařízení mohou být použity například starší telefony s Androidem. Systém FIND je volně dostupný.[1]

3.3 ProbeSniffer

Tento nástroj je určen pro odchytávání *probe-request frame* v okolí přijímače, získávání názvů výrobců zařízení odesílajících tyto WiFi rámce a ukládání odchycených dat do databáze. Aplikace v reálném čase odchytává a zobrazuje *probe-request frame* i se sílou signálu a z MAC adres se pokouší získat názvy výrobců. Výsledkem probeSniffer je zobrazení počtu WiFi zařízení v okolí přijímače. Výhodou tohoto nástroje je možnost nastavovat vlastní názvy pro MAC adresy. Pokud zařízení ve svém *probe-request frame* změní SSID sítě, kterou vyhledává, zobrazuje probeSniffer i název této sítě. Všechna nebo filtrovaná data dle MAC adresy je možné ukládat do SQLite databáze. Při použití tohoto nástroje je pro odchytávání síťového provozu nutné nainstalovat program Tshark. Dle mého názoru je toto velkou nevýhodou nástroje probeSniffer, protože pro nainstalování programu Tshark je potřeba cca 100 MB místa na disku. ProbeSniffer je volně dostupný.[2]

3.4 Howmanypeoplearearound

Také program howmanypeoplearearound určuje počet osob ve sledovaném prostoru z analýzy WiFi provozu. Osoba je prezentována WiFi zařízením, které vysílá *probe-request frame*. Využití programu je například v možnosti sledovat provoz v okolí domu. Program umožňuje exportovat sílu WiFi signálu, MAC adresu a výrobce zařízení do formátu JSON. Program skenuje WiFi provoz ve dvou režimech. V prvním režimu uživatel zadá parametr času, tzn. jak dlouho bude program odchytávat WiFi rámce. Druhý režim pracuje v nekonečné smyčce, kdy program přidává získaná data ze skenování na konec souboru. Program rovněž umožňuje jednoduchou vizualizaci dat získaných z obou režimů. Na lokální stanici program vytvoří webový server, na kterém se zobrazují výsledky skenování v podobě grafů. Grafy zobrazují počet nalezených WiFi zařízení v konkrétních časech, jejich sílu signálu a jednotlivé MAC adresy. Stejně jako u nástroje probeSniffer, jsou data ze síťového adaptéru získávána z programu Tshark, což několikanásobně zvyšuje potřebu místa na disku, než je potřeba samotného programu (pozn. program má velikost 5 MB). Rovněž program howmanypeoplearearound je volně dostupný.[3]

[1] https://github.com/schollz/find
[2] https://github.com/xdavidhu/probeSniffer
[3] https://github.com/schollz/howmanypeoplearearound

3.5 Indoor GPS

Indoor GPS je aplikace určená pro operační systém Android od verze 3 a výše. Aplikace je využívána pro navigování osob nejen ve volném prostoru, ale i v budovách. Podmínkou pro použití aplikace Indoor GPS je nahrání plánu prostoru nebo budovy do této aplikace. Následně v nahraném plánu označíte, kde se právě nacházíte. Po přemístění na druhou lokaci tuto lokaci v aplikaci opět označíte. Následně se přemístíte na třetí lokaci, kterou v aplikaci označíte jako konečnou. Poté co změníte lokaci, aplikace podle síly signálu AP zobrazí v plánu místo, kde se právě nacházíte. Výhoda této aplikace spočívá v tom, že k určován polohy zařízení potřebuje aplikace pouze WiFi signály AP. Aplikace tudíž může být využívána i v prostorách, kde není GPS pokrytí. Program Indoor GPS je volně dostupný.[4]

[4] https://play.google.com/store/apps/details?id=com.ladiesman217.indoorgps&hl=en

4 Popis aplikace

Pro zpracování bakalářské aplikace jsem si v souladu se zadáním bakalářské práce vybral metodu, která pracuje na bázi pasivního skenování WiFi kanálů. To znamená, že síťový adaptér bude data pouze přijímat, ale žádná data nebude nevysílat. Síťový adaptér v danou chvíli skenuje na jednom WiFi kanále pouze příchozí signály a po uplynutí časového intervalu přechází na skenování jiného kanálu. Aplikace odchytává WiFi rámce zařízení nacházejících se v rádiovém dosahu přijímače, poté je analyzuje, případně může výsledky zpracovat do grafů i protokolu. Analýza odchycených WiFi rámců může být zpracovávána dle různých požadavků volbou vhodných parametrů. Bakalářská aplikace umožňuje odchytávání WiFi rámců a jejich analýzu na jiném zařízení, než na kterém bude probíhat generování grafů, případně protokolu. Aplikace pracuje s předpokladem, že jedna osoba má právě jedno WiFi zařízení s jednou unikátní MAC adresou.

4.1 Implementace aplikace

Odhadování počtu osob bakalářskou aplikací je založeno na odchytávání WiFi rámců zařízení nacházejících se v rádiovém dosahu přijímače, které analyzuje a v případě požadavku může výsledky zpracovat do grafů a protokolu. Dle tohoto je aplikace rozdělena na dvě komponenty. První komponenta zajišťuje sběr odchycených WiFi rámců ze síťového rozhraní, jejich analýzu a výsledný export do formátu csv. Tato část aplikace je naprogramována v programovacím jazyku Pythonu. Druhá komponenta zajišťuje vytvoření příslušných grafů z exportovaných dat s využitím jazyka R. Uživatel má možnost výsledky skenování vygenerovat do protokolu, který jsem vytvořil v LaTeXu a je nutné jej spustit manuálně.

4.1.1 Sběr dat

Bakalářská aplikace může pracovat ve dvou režimech. V prvním režimu aplikace začne ihned po spuštění analyzovat všechny odchycené WiFi rámce. Tento režim je vhodný v případech, kdy je potřeba odhadnout celkový počet zařízení v okolí přijímače. Druhý režim je vhodný v případech, kdy potřebujeme zjistit, kolik zařízení, resp. osob v okolí přijímače přibylo v určitém časovém intervalu. Ve druhém režimu si aplikace nejdříve uloží MAC adresy zařízení, která po zvolenou dobu (stadium učení) vysílají. Tyto MAC adresy jsou nežádoucí pro výsledky počtů osob, a proto se s těmito adresami již dále nepočítá. Po skončení stadia učení aplikace začne s odchytáváním a analýzou nově odchycených WiFi rámců, avšak pouze těch, které neobsahují nežádoucí MAC adresy zařízení, které byly vysílány v době stadia učení.

Konečné výsledky skenování WiFi provozu mohou být ovlivněny různými parametry, které si uživatel zvolí v nastavení aplikace. Uživatel aplikace má tak možnost nastavit např. parametr na filtrování typů WiFi rámců zařízení, která jsou uživatelem označená jako vyloučená pro výsledky z hlediska počtu osob, jako např. *beacon frame*, které vysílá AP. Použitím vhod-

ných parametrů tudíž dojde ke zpřesnění výsledků. Parametrům se věnuji v podkapitole 4.3.1 Nastavení aplikace.

Bakalářská aplikace je rozdělena do pěti níže uvedených souborů:

- run.py – hlavní část aplikace zajišťující sběr a analýzu odchycených WiFi rámců; zároveň se o jedná spouštěcí soubor aplikace
- settings.py – soubor zajišťující nastavení parametrů pro skenování, jako např. výběr síťového adaptéru nebo výběr skenovaných kanálů
- oui.py – soubor, který obsahuje dvojice OUI a název výrobce, kterému dané OUI náleží
- subtypes.py – soubor, který obsahuje typy WiFi rámců
- graphexport.R – soubor, který vygeneruje z výstupu aplikace příslušné grafy
- protocol.tex – šablona pro generování protokolu

Po spuštění aplikace se funkcí SetupExportFolder() vytvoří složka pro exportování dat. Název této složky je tvořen z konstanty export- a unixového času spuštění programu (UNIX čas je počet sekund od 1. ledna 1970). V této složce se dále vytvoří složka Device pro export souborů s informacemi o počtu WiFi zařízeni, složka Full pro export souborů s celkovými odchycenými daty, složka StackBar pro export souborů s daty pro sloupcový graf a složka Vendor pro exportovaní souboru s daty pro výsečový graf.

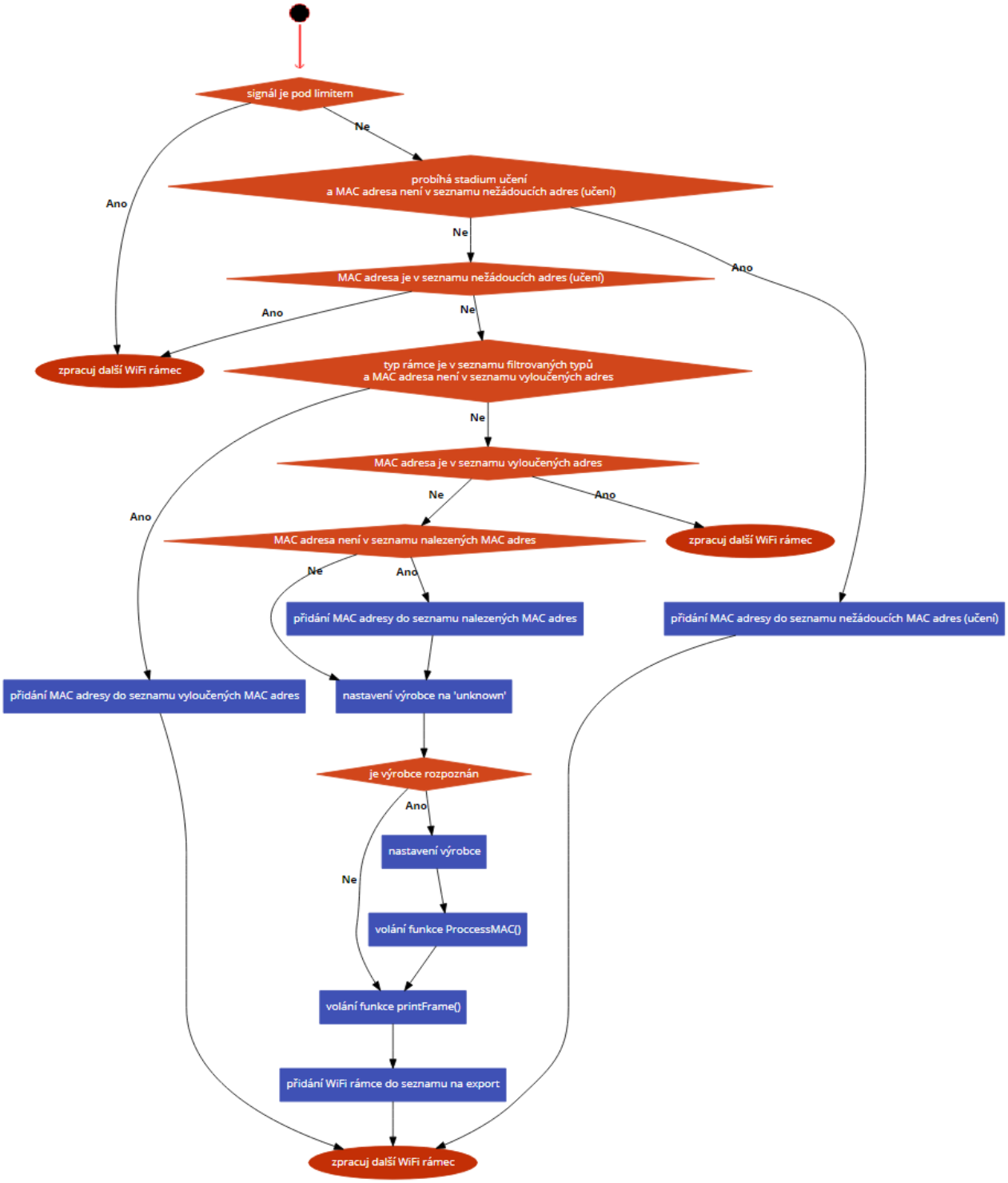
Po vytvoření složek dojde k přepnutí síťového adaptéru do *monitor mode* a začne odchytávání WiFi rámců. Po odchycení WiFi rámce se rámec otestuje, zda se jedná o *managment frame*, *control frame* nebo *data frame*. Pokud se jedná o jeden z těchto rámců, je rámec zpracován funkcí ProcessFrame(record).

4.1.2 Analýza dat

Funkce ProcessFrame(record) provádí samotnou analýzu WiFi rámce. Nejprve aplikace testuje, zda odchycený WiFi rámec nemá sílu přijatého signálu menší, než je uživatelem stanovené minimum. Dále se testuje, zda se aplikace nachází ve stadiu učení a zároveň, zda seznam nežádoucích MAC adres již neobsahuje tuto zachycenou MAC adresu zařízení. Dále se testuje, zda odchycená MAC adresa WiFi rámce nebyla odchycena ve stadiu učení. V případě, že uživatel zapne aplikaci v prvním režimu, tudíž neproběhne stadium učení, vznikne prázdný seznam nežádoucích MAC adres. Dále aplikace kontroluje, zda typ odchyceného WiFi rámce není v seznamu vyloučených typů. Poté se zkontroluje, zda MAC adresa zařízení není v seznamu zařízení, které v minulosti vyslalo jeden z filtrovaných typů WiFi rámce. Vývojový diagram funkce ProcessFrame(record) uvádím v obrázku č. 3.

Pokud odchycený WiFi rámec do této chvíle prošel všemi podmínkami, proběhne jeho analýza. V případě, že aplikace MAC adresu zařízení ještě neodchytila, přidá ji do seznamu MAC

adres počítaných osob. Pokud se z MAC adresy podaří zjistit výrobce, je název výrobce a MAC adresa zpracována funkcí ProcessMac(mac,manufacter), která má za úkol zvyšovat počítadla pro výrobce nalezených zařízení. Pokud se výrobce zařízení z MAC adresy zjistit nepodaří, je automaticky výrobci přiřazen název unknown. Odchycený WiFi rámec se poté pošle na výstup konzole a přidá se do seznamu na export.



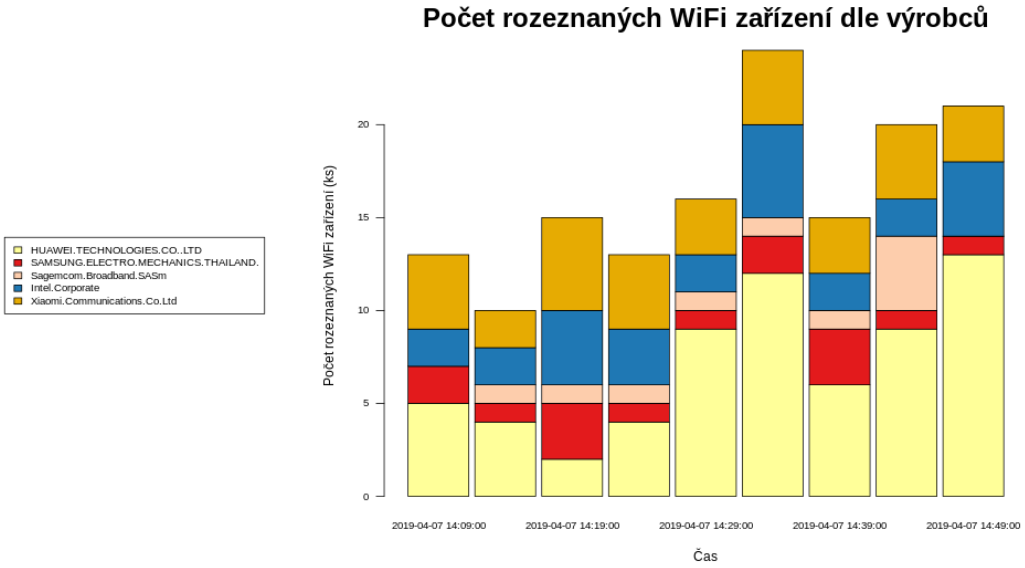
Obrázek 3: Vývojový diagram funkce ProcessFrame(record)

4.1.3 Výstup dat

V případě, že byla uživatelem v parametru generate_graph zvolena možnost s generováním výsledků do grafů, budou výsledky skenování přehledně zpracovány pomocí R skriptu do různých typů grafů ve chvíli, kdy je práce aplikace uživatelem ukončena klávesovou zkratkou **ctrl + c**. Zároveň však upozorňuji, že grafy je možné manuálně vygenerovat i v průběhu skenování.

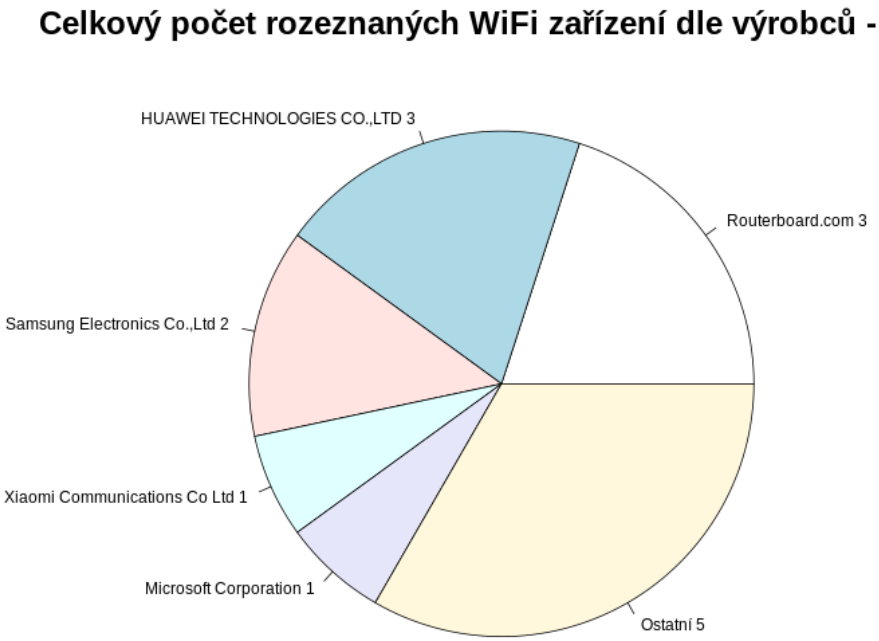
Grafy R skript vytváří na základě vygenerovaných csv souborů. Při volání R skriptu je potřeba zadat vstupní argument, a to absolutní cestu k export složce. Po spuštění si skript načte všechny potřebné soubory z export složky a vytvoří z dat příslušné grafy.

Jako první se vygeneruje graf, který prezentuje počty rozeznaných WiFi zařízení nalezených v uživatelem zvolených časových intervalech, a to dle jednotlivých výrobců (obrázek č. 4). Pro přehlednost má každý výrobce samostatné barevné označení. Osa X zobrazuje časové intervaly a osa Y zobrazuje počty nalezených a zároveň rozeznaných WiFi zařízení v kusech.



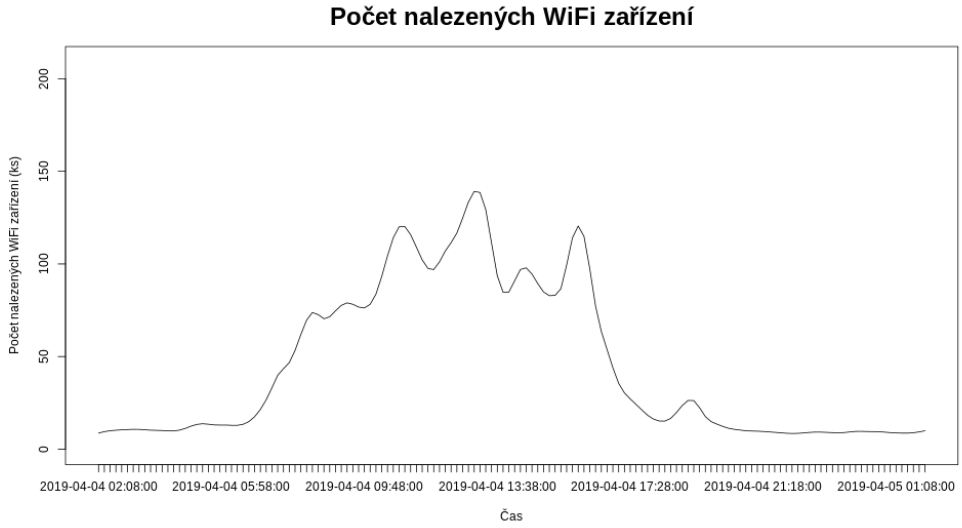
Obrázek 4: Ukázka generovaného grafu – Počet rozeznaných WiFi zařízení dle výrobců

Jako druhý v pořadí se vygeneruje výsečový graf, který zobrazuje celkové počty WiFi zařízení jednotlivých rozpoznaných výrobců nalezených bakalářskou aplikací za celou dobu sběru dat (obrázek č. 5). Každá jednotlivá výseč označuje jednoho výrobce zařízení. U výseče je vždy uvedeno jméno výrobce, kterého daná výseč znázorňuje a počet jeho nalezených zařízení. Tento graf je přehledný v případě nalezení WiFi zařízení s menším počtem výrobců. Nevýhoda tohoto grafu se projeví v případě, kdy je výrobců velký počet. Jména výrobců a počet jeho nalezených zařízení se v tomto případě začnou v grafu překrývat a jsou nečitelná. Z tohoto důvodu v případě zachycení WiFi rámců zařízení od více než šesti výrobců, vygeneruje aplikace výsečový graf, který znázorňuje počet nalezených WiFi zařízení u pěti nejčastějších výrobců a celkový počet nalezených WiFi zařízení ostatních rozpoznaných výrobců.



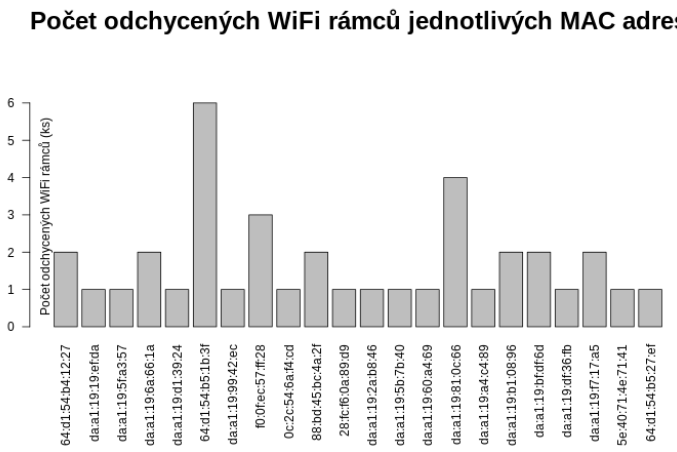
Obrázek 5: Ukázka generovaného grafu – Celkový počet rozeznaných WiFi zařízení dle výrobců – top 5

Dále se do spojnicového grafu vygeneruje počet nalezených WiFi zařízení (obrázek č. 6). Tento graf zobrazuje počty všech WiFi zařízení nalezených v daných časových intervalech, tzn. i těch, u kterých se nepodařilo zjistit výrobce. Osa X zobrazuje časové intervaly a osa Y zobrazuje počty všech nalezených WiFi zařízení v kusech. V případě tohoto grafu je z estetických důvodu prováděno mírné zaoblení výsledné křivky.



Obrázek 6: Ukázka generovaného grafu – Počet nalezených WiFi zařízení

Jako čtvrtý graf je generován graf sloupcový, který zobrazuje počet odchycených WiFi rámců jednotlivých MAC adres (obrázek č. 7). Osa X zobrazuje jednotlivé odchycené MAC adresy zařízení a osa Y zobrazuje příslušným sloupcem nad MAC adresou počet jejich odchycených WiFi rámců v kusech. U tohoto grafu se při velkém počtu MAC adres projeví stejná nevýhoda jako u výsečového grafu. Při velkém počtu MAC adres se stane graf nečitelným. Z tohoto důvodu v případě, že jsou zachyceny WiFi rámce od více než šedesáti zařízení, vygeneruje aplikace sloupcový graf, který znázorňuje počet odchycených WiFi rámců u šedesáti nejčastěji odchycených MAC adres.



Obrázek 7: Ukázka generovaného grafu – Počet odchycených WiFi rámců jednotlivých MAC adres

4.1.4 Protokol k bakalářské aplikaci

Pro přehlednost jsem k bakalářské aplikaci vytvořil v LaTeXu šablonu. Uživatel má tak možnost vygenerované grafy vložit do protokolu. Soubor na vytvoření protokolu má název protocol.tex. Generování protokolu je nutné spustit manuálně.

4.2 Instalace aplikace

Pro správnou funkci bakalářské aplikace je nutné nainstalovat potřebné knihovny. V následujícím popisu je uveden postup pro instalaci knihoven pro čistou instalaci operačního systému Ubuntu ve verzi 18.04, kdy probíhá sběr dat s analýzou i výstup na jednom zařízení.

Linux: Před instalací požadovaných modulů aktualizujeme operační systém Linux na poslední aktuální verzi. Nejprve aktualizujeme balíčkový seznam z repozitáře Linuxu příkazem **sudo apt-get update**. Tímto příkazem dojde pouze k aktualizaci seznamu, a nikoliv k aktualizaci samotných balíčků. Poté provedeme aktualizaci balíčků příkazem **sudo apt-get upgrade**. Nakonec je nutné provést aktualizaci příkazem **sudo apt-get dist-upgrade**.

PIP: Nejdříve je potřeba nainstalovat pip, což je balíčkový manažer pro programovací jazyk Python. Pip nainstalujeme příkazem **sudo apt install python-pip**.

DPKT: DPKT je modul programovacího jazyka Python pro základní parsování TCP/IP protokolu. Nainstaluje se příkazem **sudo pip install dpkt**.

Pcapy: Pro odchyt síťového provozu je použit modul Pcapy a nainstaluje se příkazem **sudo apt-get install python-pcapy**.

R: Pro správné vykreslování grafů je potřeba nainstalovat programovací jazyk R příkazem **sudo apt-get install-rbase**. Poté spustíme terminál s příkazem **R**. Nainstalování knihovny RColorBrewer příkazem **install.packages("RColorBrewer")** zajistí barevné znázornění grafů. Nakonec nainstalujeme příkazem **install.packages("anytime")** knihovnu Anytime, která je nutná pro konverzi UNIX času. Nyní je již aplikace připravena ke spuštění.

Bakalářská aplikace umožňuje sběr dat na jiném zařízení, než na jakém bude probíhat výstup dat. Toto rozdělení funkcí je výhodné z hlediska potřeb technického vybavení, protože sběr a analýza dat nemusí probíhat na velkém a výkoném zařízení. Další výhodou tohoto postupu je, že přístup ke zpracovaným výsledkům je pro uživatele pohodlnější, neboť může být přeneseno do zázemí uživatele.

Jako příklad instalace aplikace s oddělením sběru dat a výstupu uvádím případ, kdy sběr dat bude probíhat na vývojové desce ALIX s použitím operačního systému např. OpenWrt a výstup dat bude probíhat na výkonnějším zařízení (např. notebook) s operačním systémem Ubuntu

ve verzi 18.04. OpenWrt je Linuxový operační systém pro *embedded* zařízení. Jeho výhodou jsou nízké nároky na velikost paměti pro instalaci. Tento operační systém podporuje také staré procesory. Po nainstalování aktuální verze OpenWrt 18.06 je potřeba pro sběr dat nainstalovat na vývojovou desku programovací jazyk Python příkazem **opkg install python**, modul Pcapy příkazem **opkg install python-pcapy** a modul DPKT příkazem **opkg install dpkt**. Protože se grafy budou generovat na jiném zařízení, než na kterém bude probíhat sběr a zpracování WiFi rámců, je nutné v souboru settings.py vypnout generování grafů. Generování grafů se v operačním systému Ubuntu spouští manuálně.

4.3 Spuštění aplikace

V tuto chvíli již máme nainstalovány všechny potřebné prerekvizity pro spuštění bakalářské aplikace. Nyní zbývá zvolit požadované parametry a aplikaci spustit.

4.3.1 Nastavení aplikace

Aplikace pracuje s několika parametry, kterými je možné ovlivnit analýzu odchycených WiFi rámců a tím výsledek skenování. Před spuštěním aplikace si tedy uživatel musí nastavit v souboru settings.py. parametry dle konkrétního využití aplikace. Settings.py obsahuje:

- interface – zde je nutné zadat jméno síťového rozhraní, na kterém bude probíhat skenování. Výpis všech bezdrátových síťových zařízení provedeme příkazem **iwconfig -a**
- monitor_enable – příkaz pro přepnutí sítového rozhraní do *monitor mode*
- monitor_disable – příkaz pro přepnutí síťového rozhraní zpět do *managed mode*
- change_channel – příkaz pro změnu skenovaného WiFi kanálu
- channels – seznam WiFi kanálů ke skenování; při zadávání více hodnot u tohoto parametru je nutné tyto hodnoty oddělit čárkou
- sub_type_filter – seznam filtrovaných WiFi rámců, které identifikují routery, AP atd.; při zadávání více hodnot u tohoto parametru je nutné tyto hodnoty oddělit čárkou
- rssi_level_filter – dolní hranice síly WiFi signálů pro odchycení (dosah skenování)
- learning – volba stadia učení. Při zvolení možnosti True proběhne stadium učení, kdy bude aplikace skenovat WiFi provoz po dobu zvolenou v learning_interval. WiFi rámce odchycené v době stadia učení nebudou započítávány do statistik. Při volbě možnosti False neproběhne stadium učení.
- learning_interval – doba v minutách, po kterou bude aplikace naplňovat seznam nežádoucí zařízení (doba stadia učení)

- export_interval – časový interval v minutách, po kterých bude aplikace seskupovat data
- generate_graph – volba generování grafů. Při zvolení možnosti True proběhne po ukončení aplikace generování výstupu do grafů. Při volbě možnosti False ke generování výstupu do grafů nedojde.

Příklad konfigurace souboru settings.py uvádím ve výpisu č. 1. V tomto případě bude sběr odchycených dat probíhat na síťovém adaptéru s názvem wlo1, skenovat se budou pouze kanály č. 6 a 10, síla odchyceného WiFi signálu musí být menší než -120 dBm, bez stadia učení a nebudou generovány grafy.

```
interface = 'wlo1'
monitor_enable = 'sudo service network-manager stop;sudo ifconfig wlo1 down;
    sudo iwconfig wlo1 mode monitor;sudo ifconfig wlo1 up'
monitor_disable = 'sudo ifconfig wlo1 down;sudo iwconfig wlo1 mode Managed;sudo
     ifconfig wlo1 up;sudo service network-manager start'
change_channel = 'iw dev wlo1 set channel %s'
channels = [6,10]
sub_type_filter=[]
rssi_level_filter = -120
learning = False
learning_interval = 3
export_interval = 1
generate_graph = False
```

Výpis 1: Příklad konfigurace souboru settings.py

4.3.2 Start aplikace

Nyní je již bakalářská aplikace připravena k provozu. Spuštění aplikace probíhá příkazem v terminálu **sudo python run.py**. Výpis do konzole zobrazuje odchycené WiFi rámce. Aplikace odchytává WiFi rámce do okamžiku, než ji uživatel zastaví kombinací kláves **ctrl + c**. Po zastavení aplikace se síťový adaptér přepne zpět do *managed mode* a pokud je zapnuto generování grafů, vygenerují se výstupy.

Jak jsem již dříve uvedl, v případě, že sběr dat probíhá na jiném zařízení než generování výstupů, je třeba spustit generování grafů manuálně. Spouštění skriptu na generování grafů probíhá příkazem **sudo Rscript graphexport.r *PATH***, kde *PATH* je absolutní cesta k export složce (např. /home/tom/export-1555159421.49).

Příkazem **pdflatex protocol.tex** se vygenerují výsledky do protokolu za podmínky, že soubor protocol.tex je umístěn ve složce s grafy.

5 Testování bakalářské aplikace

Bakalářskou aplikaci jsem prověřil několika testy, kterým se věnuji v této kapitole. Celkem jsem provedl šest testů. Cílem testů bylo prověřit bakalářskou aplikaci z hlediska funkčnosti, úspěšnosti a správnosti počtů nalezených WiFi zařízení nebo rozpoznaných výrobců. Aplikaci jsem otestoval i z hlediska střednědobého provozu.

5.1 Test úspěšnosti zachytávání WiFi rámců

Účelem tohoto testu bylo zjistit, kolik WiFi rámců bakalářská aplikace zachytí v porovnání s jinou aplikací a zda následná analýza zachycených WiFi rámců má vliv na celkový počet odchycených WiFi rámců. Pro toto testování jsem použil notebook, na kterém byla spuštěna bakalářská aplikace a zároveň program Wireshark[5] (program pro odchycení a analýzu síťových protokolů). Bakalářskou aplikaci jsem zároveň spustil i na RB. Výsledky z obou zařízení jsem porovnal vždy po pěti minutách. Pro účely tohoto testu považuji počty WiFi rámců odchycených programem Wireshark za maximálně možný počet odchycených WiFi rámců. Odchytávání WiFi rámců probíhalo pouze na kanále č. 6. V první části tohoto testu bakalářská aplikace při zachycení WiFi rámce pouze přičetla k čítači jedničku, aniž by WiFi rámec dále analyzovala. Ve druhé části tohoto testu došlo již k analýze odchycených WiFi rámců.

Čas (min)	Wireshark	%	Aplikace na notebooku	%	Aplikace na RB	%
5	27.921	100%	27.864	99,79%	26.129	93,58%
10	35.726	100%	35.680	99,87%	31.579	88,39%
15	43.523	100%	43.497	99,94%	38.957	87,50%
20	47.638	100%	47.556	99,82%	40.814	85,67%
25	54.227	100%	54.069	99,70%	46.263	85,31%
30	62.272	100%	62.095	99,71%	53.768	86,34%

Tabulka 3: Počty odchycených WiFi rámců bez analýzy v ks

Výsledek: Z údajů v tabulce č. 3 je zřejmé, že bakalářská aplikace nezachytila všechny WiFi rámce, které zachytil program Wireshark. Rozdíl v počtu odchycených WiFi rámců může být způsoben v rozdílném časovém okamžiku, kdy začnal samotný odchyt WiFi rámců bakalářskou aplikací a programem Wiresharku. Další možný důvod je v implementaci knihovny Pcapy. Nižší počet WiFi rámců odchycených bakalářskou aplikaci nainstalovanou na RB je zřejmě způsobeno rozdílným ziskem antény.

Z údajů v tabulce č. 4 je zřejmé, že na počet odchycených WiFi rámců nemělo vliv zpracovávání jejich analýzy, tzn. bakalářská aplikace provádí analýzu WiFi rámců s dostatečnou rychlostí.

[5] https://www.wireshark.org/

Čas (min)	Wireshark	%	Aplikace na notebooku	%	Aplikace na RB	%
5	3.015	100%	2.989	99,13%	2.797	92,76%
10	10.626	100%	10.572	99,49%	8.437	79,39%
15	16.758	100%	16.651	99,36%	14.327	89,49%
20	20.320	100%	20.197	99,39%	18.938	93,19%
25	26.977	100%	26.783	99,28%	24.572	91,08%
30	31.542	100%	31.316	99,28%	29.942	94,92%

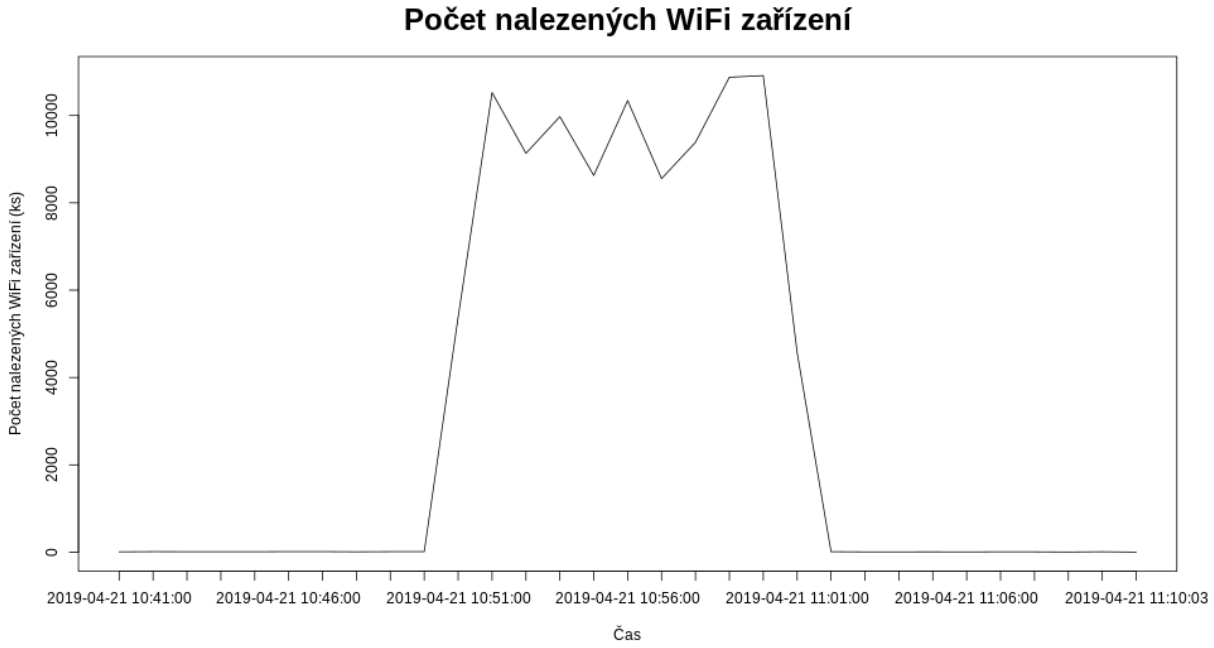
Tabulka 4: Počty odchycených WiFi rámců s analýzou v ks

5.2 Test s falešnými WiFi rámci

Problematika programů, které mají za úkol oklamat počítadla osob tím, že generují náhodné *probe request frame* na náhodně vygenerovaném kanálu, mne vedla k potřebě otestovat bakalářskou aplikaci také z hlediska tzv. falešných WiFi rámců. Programy na čítání osob náhodně vygenerované WiFi rámce zachytí a započítají do výsledku i přes to, že jsou falešné. Z tohoto důvodu programy, které čítají osoby podle získaných MAC adres, mohou vykazovat vyšší počty osob, než je jejich skutečný počet. Pro testování jsem použil program VALORA – WiFi Tracker Confuser stažený z GitHubu[6] nainstalovaný na NodeMcu[7]. Bakalářskou aplikaci jsem spustil bez stadia učení. Po cca deseti minutách skenování jsem spustil program VALORA – WiFi Tracker Confuser, který vysílal falešné WiFi rámce dalších 10 minut. Poté jsem program VALORA – WiFi Tracker Confuser vypnul, ale bakalářská aplikace WiFi provoz skenoval dalších cca 10 minut. Očekávám, že v čase, kdy program VALORA – WiFi Tracker Confuser odesílal falešné WiFi rámce, zaznamená bakalářská aplikace vysoký počet nalezených WiFi zařízení.

[6] https://github.com/antoinet/valora/

[7] https://www.nodemcu.com/index_en.html/



Obrázek 8: Počet nalezených WiFi zařízení ovlivněný falešnými WiFi rámci

Výsledek: Z výsledku grafu v obrázku č. 8 je zřejmé, že program VALORA – WiFi Tracker Confuser úspěšně oklamal bakalářskou aplikaci, která vykázala nereálný počet nalezených WiFi zařízení.

5.3 Test randomizace MAC adresy

V testu randomizace MAC adres jsem se věnoval problematice algoritmů, které mají za úkol snížit možnosti sledování zařízení během hledání dostupných WiFi sítí. Algoritmus zařízení pracuje na principu periodické změny MAC adresy během hledání WiFi sítě. Programy čítající osoby nebo sledující jejich polohu ovlivňuje tím, že každou změněnou adresu program detekuje jako novou osobu, čímž dochází ke zkreslování výsledků. Ve skutečnosti je ve sledovaném prostoru méně zařízení, než kolik je odchycených MAC adres. Toto jsem se pokusil ověřit testem randomizace MAC adresy. Test probíhal 60 minut s mobilním telefonem Huawei P Smart s nainstalovaným operačním systémem Android 8.0 Oreo. Telefon měl po celou dobu testu zapnutý displej se seznamem dostupných WiFi sítí, k žádné WiFi síti však nebyl připojen. Bakalářská aplikace měla nastavenou hodnotu signálu pod -30 dBm, aby odchytávala WiFi rámce pouze z tohoto zařízení. Skutečná MAC adresa telefonu je 24:2e:02:30:f0:fe.

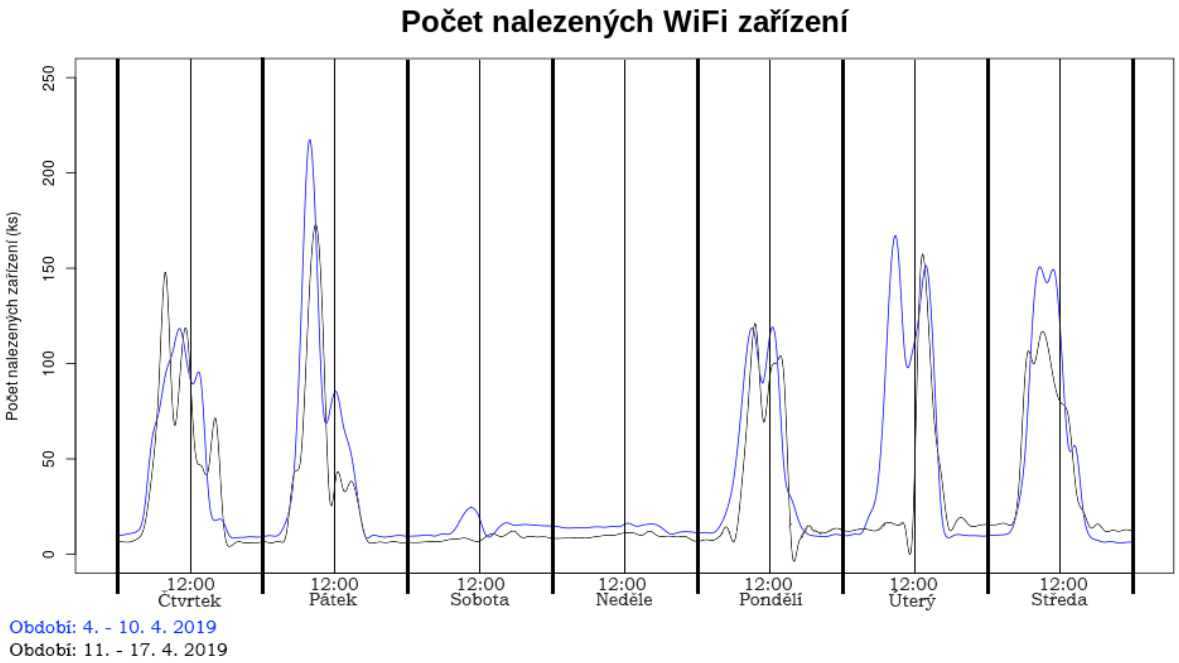
Výsledek: Dle předpokladů mobilní telefon měnil periodicky svou MAC adresu při hledání WiFi sítí. V průběhu hodinového hledání vygenerovalo zařízení celkově 377 MAC adres, což je 6,2 MAC adres za 1 minutu hledání. Během hledání však zařízení nepoužilo ani jednou svou pravou MAC adresu. Všechny generované MAC adresy obsahovaly stejné OUI (da:a1:19), které však nepatří žádnému výrobci. V generovaných MAC adresách se měnily hodnoty NIC.

Jelikož byly MAC adresy unikátně vygenerovány, bakalářská aplikace je odchytila a detekovala jako MAC adresy nových zařízení. Byly tedy připočteny do celkového počtu nalezených WiFi zařízení. Výsledkem sledování mělo být nalezení jednoho zařízení, a to od výrobce HUAWEI TECHNOLOGIES CO.,LTD. Aplikace však vykázala 377 nalezených zařízení od neznámého výrobce. Níže uvádím prvních deset odchycených MAC adres:

- da:a1:19:0e:07:60
- da:a1:19:84:5d:b5
- da:a1:19:48:bd:94
- da:a1:19:b8:e3:7d
- da:a1:19:44:16:2a
- da:a1:19:86:ad:4c
- da:a1:19:6e:24:eb
- da:a1:19:3e:ac:e4
- da:a1:19:3f:ff:38
- da:a1:19:62:6c:63

5.4 Střednědobé sledování WiFi provozu

Následujícím testem jsem bakalářskou aplikaci vyzkoušel ve střednědobém sledování WiFi provozu na frekventovaném místě. Pro tento test jsem aplikaci nainstaloval na RB, který jsem umístil v budově VŠB-TUO v učebně katedry FEI. Bakalářská aplikace skenovala WiFi provoz v učebně a blízkém okolí v období od 4. 4. 2019 0.00 hod. do 17. 4. 2019 24.00 hod. Při testování jsem očekával, že v jednotlivých časových okamžicích bude kolísat počet nalezených WiFi zařízení v závislosti s proměnlivou hustotou užívání sledovaných prostorů. Při testování by se měl projevit markantní rozdíl v počtech WiFi zařízení nalezených v denních a nočních hodinách, kdy v nočních hodinách bude počet nalezených WiFi zařízení minimální. Aplikace bude odchycená data průběžně zaznamenávat do spojnicového grafu, čímž bude možné sledovat vývoj odchycených dat již v průběhu testování. Na ose X budou uvedeny názvy dnů a na ose Y počet nalezených WiFi zařízení, tzn. že graf hodnot z prvního týdne testování se bude překrývat s grafem hodnot z druhého týdne. Takto získáme přehledné zobrazení výsledků testování.



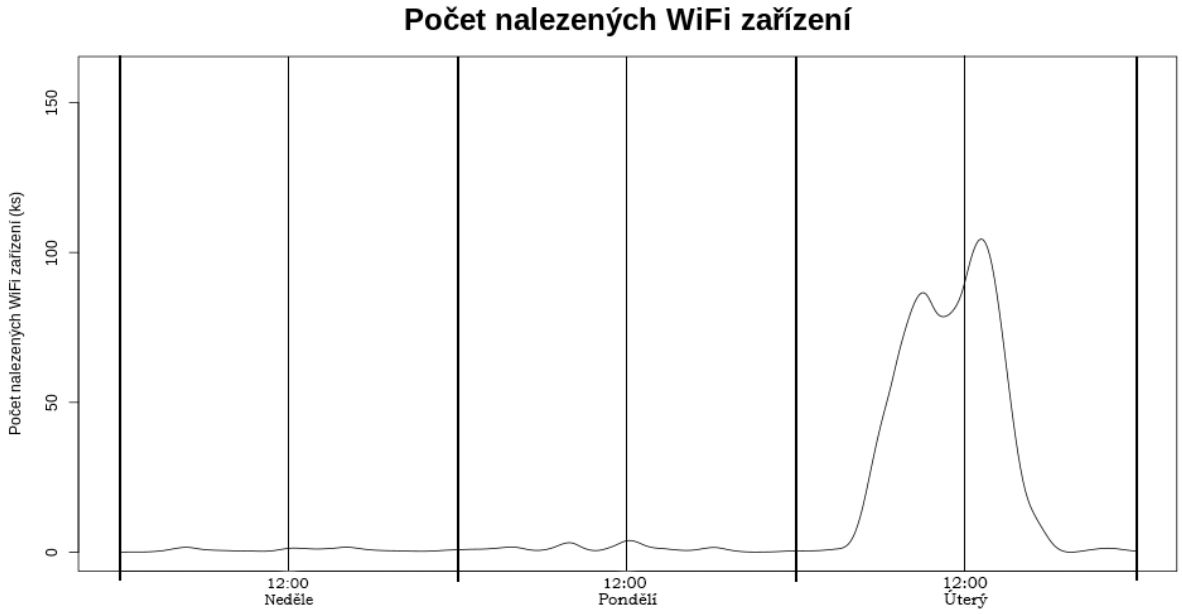
Obrázek 9: Počet nalezených WiFi zařízení při střednědobém testu

Výsledek: Z údajů grafu v obrázku č. 9 je zřejmé, že vývoj počtů WiFi zařízení nalezených v průběhu prvního týdne je velmi podobný vývoji počtů WiFi zařízení nalezených v průběhu druhého týdne. V souladu s očekáváním došlo v průběhu sledovaného období i v průběhu jednotlivých dní ke kolísání počtu nalezených WiFi zařízení. Největší počet nalezených WiFi zařízení bakalářská aplikace zaznamenala v časech, kdy ve sledovaném prostoru probíhaly přednášky a cvičení. Nejmenší počet nalezených WiFi zařízení byl zaznamenán o víkendech a po celý týden v nočních hodinách. V tuto dobu byl počet nalezených zařízení minimální, ne však nulový, jak by mohl někdo očekávat. Tento stav zřejmě nebyl způsoben tím, že by se v budově nacházela osoba s WiFi zařízením nebo se v ní nacházelo nějaké zapomenuté WiFi zařízení. Na základě svých znalostí sledovaných prostor soudím, že v nočních hodinách zachycené WiFi rámce vysílala trvale umístěná zařízení v budově jako např. meteostanice. V počtu nalezených WiFi zařízení může být rovněž zahrnut i nevypnutý počítač s WiFi síťovým adaptérem. Tento test potvrdil, že bakalářská aplikace pracovala i při střednědobém sledování WiFi provozu bez potřeby údržby (restartování aplikace), což považuji za její výhodu.

5.5 Test se stadiem učení

Na základě výsledků testu Střednědobého sledování WiFi provozu jsem otestoval aplikaci s režimem učení v nočních hodinách. Při testování jsem očekával, že poté, co aplikace uloží MAC adresy zařízení, která během učení vysílala, bude počet odchycených zařízení v nočních hodinách nulový. Dobu učení jsem zvolil na jednu hodinu, vlastní skenování WiFi provozu proběhlo v období od 21. 4. 2019 0.00 hod. do 23. 4. 2019 24.00 hod.

Výsledek: Z údajů grafu v obrázku č. 10 je zřejmé, že bakalářská aplikace se stádiem učení vyeliminovala nežádoucí statická WiFi zařízení a tudíž zaznamenala v nočních hodinách minimální počet nalezených WiFi zařízení. Tento stav pokračoval i v pondělí 22. 4. 2019, neboť se jednalo o den státního svátku a sledované prostory nebyly užívány. Zvýšený počet nalezených WiFi zařízení byl zaznamenán až v úterý 23. 4. 2019. Očekávaný nulový počet WiFi zařízení nalezených v nočních hodinách aplikace nevykázala zřejmě z důvodu, že v průběhu hodinového stadia učení tato WiFi zařízení nevysílala a tudíž nebyla jejich MAC adresa zařazena do seznamu nežádoucích MAC adres.



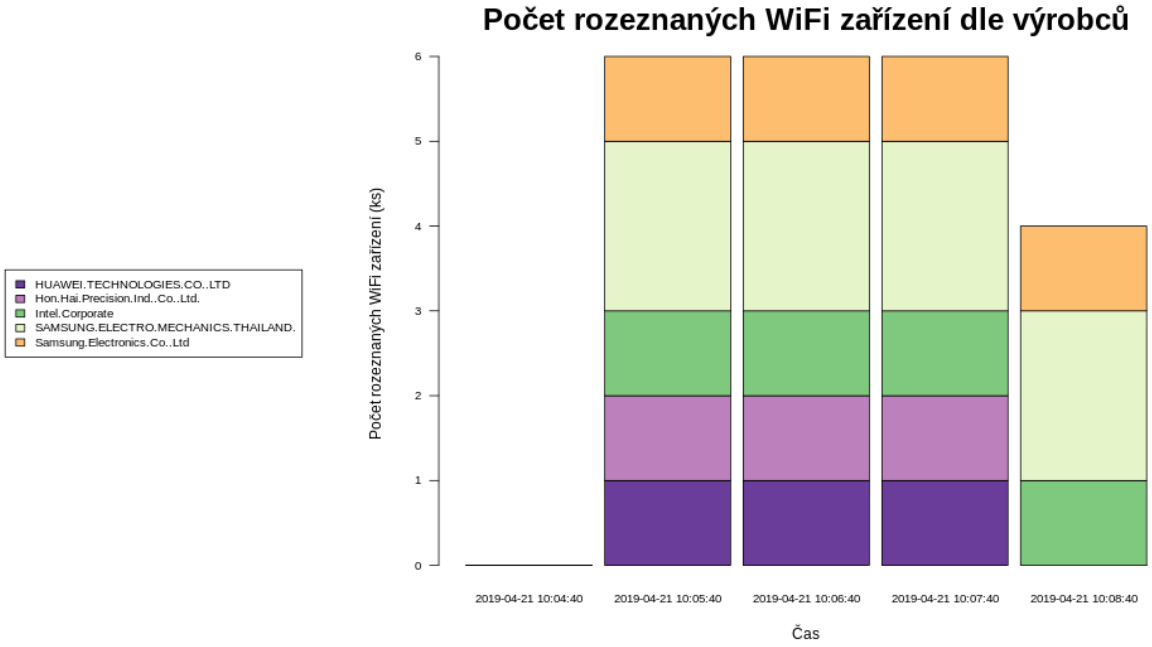
Obrázek 10: Počet nalezených WiFi zařízení s režimem učení

5.6 Test s cíleným odchytáváním WiFi zařízení

Jako poslední jsem provedl test na odchycení konkrétních WiFi zařízení. Bakalářskou aplikaci jsem spustil se stadiem učení v trvání 10 min a dobou seskupování po 1 min. Po ukončení stadia učení jsem po cca jedné minutě skenování přinesl k přijímači šest WiFi zařízení:

- 2 mobilní telefony – výrobce: Samsung
- 1 mobilní telefon – výrobce: Huawei
- 1 tablet – výrobce: Samsung
- 1 notebook – výrobce: HP
- 1 notebook – výrobce: Dell

Všechna přinesená zařízení měla zapnuté WiFi. Po dalších třech minutách jsem vypnul mobilní telefon od výrobce Huawei a notebook od výrobce HP. Od testu jsem očekával, že aplikace zaznamená 6 nalezených WiFi zařízení a následně jejich úbytek.



Obrázek 11: Počet nalezených WiFi zařízení dle výrobců s režimem učení

Výsledek: Z vygenerovaného grafu v obrázku č. 11 je zřejmé, že krátce po stadiu učení bakalářská aplikace nenalezla žádné WiFi zařízení. Po jedné minutě byla bakalářskou aplikací nalezena všechna přinesená zařízení, zároveň byly úspěšně rozeznáni výrobci těchto zařízení. Po dalších třech minutách aplikace zaznamenala úbytek dvou WiFi zařízení od výrobců Huawei a HP. Z výše uvedeného vyplývá, že test proběhl dle očekávání.

Výsledky výše uvedených testů bakalářské aplikace odpovídaly očekávaným výsledkům. Bakalářskou aplikaci by bylo možné více otestovat řízenými testy, např. kdy by do místnosti byly vpuštěny osoby, které by měli právě jedno WiFi zařízení a počet osob by byl znám.

6 Závěr

Cílem mé bakalářské práce bylo navrhnout a otestovat softwarovou aplikaci vytvořenou za účelem odhadování počtu osob v rádiovém dosahu přijímače na základě pasivní analýzy WiFi signálu, tzn. na základě odchytávání WiFi rámců odeslaných zařízeními v okolí přijímače.

Na začátku práce jsem se seznámil s technickými pojmy, principy a postupy odchytávání signálů z WiFi zařízení. Poté jsem zjišťoval, jaké softwarové aplikace na čítání osob jsou v současné době na trhu k dispozici, na jakém principu tyto aplikace pracují, zda mají také jiné možnosti vyžití a které z nich jsou volně dostupné.

Po této teoretické přípravě jsem přistoupil k tvorbě vlastní aplikace na čítání osob. Bakalářská aplikace pracuje s předpokladem, že jedna osoba má právě jedno WiFi zařízení s jednou unikátní MAC adresou. V souladu se zadáním bakalářské práce aplikace pouze pasivně skenuje konkrétní WiFi kanál, kde odchytává WiFi rámce zařízení nacházejících se v rádiovém dosahu přijímače a průběžně je analyzuje. Po uplynutí časového intervalu sítový adaptér přechází na skenování jiného WiFi kanálu a opět odchycené WiFi rámce analyzuje. Takto pokračuje do zastavení aplikace uživatelem. Analýza odchycených WiFi rámců může být zpracována dle různých požadavků uživatele volbou vhodných parametrů, např. volba síťového adaptéru, volba skenovaných kanálů nebo dolní hranice síly WiFi signálu.

Při tvorbě aplikace jsem implementoval uživateli možnost zapnout generování výsledků skenování do různých typů grafů, a to po zastavení aplikace. Zároveň má uživatel možnost již v průběhu skenování a analýzy odchycených WiFi rámců manuálně spustit generování grafů z do té doby získaných dat. Z grafů lze vyčíst různé údaje např. počet rozeznaných WiFi zařízení dle výrobců, počet všech nalezených zařízení, počet odchycených WiFi rámců jednotlivých zařízení apod. Z grafu s názvem Počet nalezených WiFi zařízení je možno vysledovat využití skenovaného prostoru v čase. Uživatel má možnost tyto grafy nechat generovat i na jiném zařízení, než na kterém probíhá odchytávání WiFi rámců a jejich analýza. K bakalářské práci jsem vytvořil v LaTeXu šablonu, která vygenerované grafy vloží do protokolu.

Bakalářskou aplikaci jsem prověřil několika testy. Z výsledků testů je zřejmé, že výsledky skenování WiFi provozu mou aplikací jsou srovnatelné s výsledky skenování programem Wireshark. Výsledky čítání aplikace však mohou být ovlivněny randomizací MAC adresy. Aplikace úspěšně prošla testem se stadiem učení a testem střednědobého provozu, kdy se ve výsledcích projevila různá hustota užívání sledovaného prostoru.

Jako výhodu mé aplikace proti aplikacím uvedeným v kapitole č. 3 považuji možnost využití stadia učení. WiFi rámce zachycené ve stadiu učení nejsou připočteny k WiFi rámcům zachyceným v době vlastního skenování. Tím dochází ke zpřesnění výsledků čítání osob v daném prostoru. Žádná z výše uvedených aplikací toto neumožňuje.

Zároveň musím konstatovat, že nevýhoda metody pasivního sledování WiFi provozu vyplývá z jejího principu fungování. V případě, že v danou chvíli na sledovaném kanále zařízení nevysílá, síťový adaptér WiFi zařízení nezachytí. Může tak nastat situace, že ve chvíli, kdy zařízení začne

vysílat a mohlo by být tudíž síťovým adaptérem nalezeno, může síťový adaptér sledovat již jiný kanál a WiFi rámec nebude zachycen. Toto možné zkreslení výsledků považuji za nevýhodu metody pasivního sledování WiFi provozu. Další nevýhodou pasivního sledování je vyšší spotřeba energie během skenování.

V závěru své bakalářské práce bych rád konstatoval, že cíl bakalářské práce vytvořit aplikaci na čítání osob na základě analýzy WiFi provozu byl splněn. Z výsledků testů bakalářské aplikace je zřejmé, že na přesnost jejích výsledků má vliv několik faktorů, např. existence zařízení bez WiFi nebo randomizace MAC adres. Aplikace je reálně použitelná spíše na sledování vytíženosti sledovaných prostorů. V případě, že použijeme více síťových adaptérů, je možné aplikaci rozšířit o možnost skenování více WiFi kanálů současně, čímž dojde k dalšímu zpřesnění výsledků skenování WiFi provozu.

Literatura

[1] *Cell Phone Tracker – How to track cell phone location guide* [online]. c2012 [citováno 17. 02. 2019]. Dostupný z WWW: https://cellphonetracker.net/gsm-tracking-introduction-to-gsm-cell-phone-tracking-its-uses-for-individuals-and-companies/

[2] ZANDL, Patrick. Bezdrátové sítě WiFi: praktický průvodce. Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-7226-632-2

[3] *Wireless Standards: 802.11a, 802.11b/g/n and 802.11ac* [online]. c2019 [citováno 22. 2. 2019]. Dostupný z WWW: https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553

[4] *What are passive and active scanning? / Wi-Fi Alliance* [online]. c2019 [citováno 05. 03. 2019]. Dostupný z WWW: https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning

[5] *802.11 Association process explained* [online]. c2018 [citováno 27. 03. 2019]. Dostupný z WWW: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_process_explained

[6] HORSKÝ, Radek. Bezdrátové sítě Wi-Fi v rekordním čase. Vyd. 1. Praha: Grada, 2006, 84 s. ISBN 80-247-1790-5

[7] *Tracking people via WiFi (even when not connected)* [online]. c2019 [citováno 10. 04. 2019]. Dostupný z WWW: https://www.crc.id.au/tracking-people-via-wifi-even-when-not-connected/

[8] *Privacy: MAC Randomization* [online]. c2018 [citováno 19. 04. 2019]. Dostupný z WWW: https://source.android.com/devices/tech/connect/wifi-mac-randomization

[9] *Enable random MAC address in Windows 10 for Wi-Fi adapter* [online]. c2018 [citováno 19. 04. 2019]. Dostupný z WWW: https://winaero.com/blog/enable-random-mac-address-in-windows-10-for-wi-fi-adapter/

[10] *iwlwifi: mvm: support random MAC address for scanning* [online]. c2018 [citováno 19. 04. 2019]. Dostupný z WWW: https://github.com/torvalds/linux/commit/effd05ac479b80641835f9126bbe93146686c2b8